



# PECB

ISO-IEC-27001-Lead-Implementer Exam

PECB ISO/IEC 27001 Lead Implementer Exam

Exam Latest Version: 9.2

## DEMO Version

### Full Version Features:

- 90 Days Free Updates
- 30 Days Money Back Guarantee
- Instant Download Once Purchased
- 24 Hours Live Chat Support

**Full version is available at link below with affordable price.**

<https://www.directcertify.com/pecb/iso-iec-27001-lead-implementer>

### Question 1. (Single Select)

Scenario 1: HealthGenic is a pediatric clinic that monitors the health and growth of individuals from infancy to early adulthood using a web-based medical software. The software is also used to schedule appointments, create customized medical reports, store patients' data and medical history, and communicate with all the involved parties, including parents, other physicians, and the medical laboratory staff.

Last month, HealthGenic experienced a number of service interruptions due to the increased number of users accessing the software. Another issue the company faced while using the software was the complicated user interface, which the untrained personnel found challenging to use.

The top management of HealthGenic immediately informed the company that had developed the software about the issue. The software company fixed the issue; however, in the process of doing so, it modified some files that comprised sensitive information related to HealthGenic's patients. The modifications that were made resulted in incomplete and incorrect medical reports and, more importantly, invaded the patients' privacy.

Based on the scenario above, answer the following question:

Which of the following indicates that the confidentiality of information was compromised?

- A: Service interruptions due to the increased number of users
- B: Invasion of patients' privacy
- C: Modification of patients' medical reports

**Correct Answer: B**

#### **Explanation:**

Confidentiality of information is the property that information is not made available or disclosed to unauthorized individuals, entities, or processes. In other words, confidentiality ensures that only those who are authorized to access the information can do so. In the scenario, the confidentiality of information was compromised when the software company modified some files that contained sensitive information related to HealthGenic's patients. This modification resulted in the invasion of patients' privacy, which means that their personal and medical information was exposed to unauthorized parties. Therefore, the correct answer is B.

## Question 2. (Single Select)

Scenario 2: Beauty is a cosmetics company that has recently switched to an e-commerce model, leaving the traditional retail. The top management has decided to build their own custom platform in-house and outsource the payment process to an external provider operating online payments systems that support online money transfers.

Due to this transformation of the business model, a number of security controls were implemented based on the identified threats and vulnerabilities associated to critical assets. To protect customers' information. Beauty's employees had to sign a confidentiality agreement. In addition, the company reviewed all user access rights so that only authorized personnel can have access to sensitive files and drafted a new segregation of duties chart.

However, the transition was difficult for the IT team, who had to deal with a security incident not long after transitioning to the e-commerce model. After investigating the incident, the team concluded that due to the out-of-date anti-malware software, an attacker gained access to their files and exposed customers' information, including their names and home addresses.

The IT team decided to stop using the old anti-malware software and install a new one which would automatically remove malicious code in case of similar incidents. The new software was installed in every workstation within the company. After installing the new software, the team updated it with the latest malware definitions and enabled the automatic update feature to keep it up to date at all times. Additionally, they established an authentication process that requires a user identification and password when accessing sensitive information.

In addition, Beauty conducted a number of information security awareness sessions for the IT team and other employees that have access to confidential information in order to raise awareness on the importance of system and network security.

Based on the scenario above, answer the following question:

After investigating the incident. Beauty decided to install a new anti-malware software. What type of security control has been implemented in this case?

- A: Preventive
- B: Detective
- C: Corrective

**Correct Answer: A**

## Explanation:

In the scenario described, Beauty's decision to install new anti-malware software after a security incident is a Preventive control. This type of control is aimed at preventing future security incidents by removing malicious code and protecting against malware infections. The purpose of the new anti-malware software is to proactively protect the company's systems and data from potential threats, thus it falls under the category of preventive measures.

ISO/IEC 27001:2022 Lead Implementer Course Guide<sup>1</sup>

ISO/IEC 27001:2022 Lead Implementer Info Kit<sup>2</sup>

ISO/IEC 27001:2022 Information Security Management Systems - Requirements<sup>3</sup>

ISO/IEC 27002:2022 Code of Practice for Information Security Controls<sup>4</sup>

What are Security Controls? | IBM<sup>3</sup>

What Are Security Controls? - F5<sup>4</sup>

### Question 3. (Single Select)

Scenario 2: Beauty is a cosmetics company that has recently switched to an e-commerce model, leaving the traditional retail. The top management has decided to build their own custom platform in-house and outsource the payment process to an external provider operating online payments systems that support online money transfers.

Due to this transformation of the business model, a number of security controls were implemented based on the identified threats and vulnerabilities associated to critical assets. To protect customers' information. Beauty's employees had to sign a confidentiality agreement. In addition, the company reviewed all user access rights so that only authorized personnel can have access to sensitive files and drafted a new segregation of duties chart.

However, the transition was difficult for the IT team, who had to deal with a security incident not long after transitioning to the e-commerce model. After investigating the incident, the team concluded that due to the out-of-date anti-malware software, an attacker gained access to their files and exposed customers' information, including their names and home addresses.

The IT team decided to stop using the old anti-malware software and install a new one which would automatically remove malicious code in case of similar incidents. The new software was installed in every workstation within the company. After installing the new software, the team updated it with the latest malware definitions and enabled the automatic update feature to keep it up to date at all times. Additionally, they established an authentication process that requires a user identification and password when accessing sensitive information.

In addition, Beauty conducted a number of information security awareness sessions for the IT team and other employees that have access to confidential information in order to raise awareness on the importance of system and network security.

Which statement below suggests that Beauty has implemented a managerial control that helps avoid the occurrence of incidents? Refer to scenario 2.

A: Beauty's employees signed a confidentiality agreement

B: Beauty conducted a number of information security awareness sessions for the IT team and other employees that have access to confidential information

C: Beauty updated the segregation of duties chart

**Correct Answer: B**

#### **Explanation:**

Managerial controls are administrative actions that are designed to prevent or reduce the likelihood of security incidents by influencing human behavior. They include policies, procedures, guidelines, standards, training, and awareness programs. In scenario 2, Beauty has implemented a managerial control by conducting information security awareness sessions for the IT team and other employees that have access to confidential information. These sessions aim to educate the staff on the importance of system and network security, the potential threats and vulnerabilities, and the best practices to follow to avoid the occurrence of incidents. By raising the level of awareness and knowledge of the employees, Beauty can reduce the human errors and negligence that might compromise the security of the information assets.

#### **Question 4. (Single Select)**

Scenario 2: Beauty is a cosmetics company that has recently switched to an e-commerce model, leaving the traditional retail. The top management has decided to build their own custom

platform in-house and outsource the payment process to an external provider operating online payments systems that support online money transfers.

Due to this transformation of the business model, a number of security controls were implemented based on the identified threats and vulnerabilities associated to critical assets. To protect customers' information. Beauty's employees had to sign a confidentiality agreement. In addition, the company reviewed all user access rights so that only authorized personnel can have access to sensitive files and drafted a new segregation of duties chart.

However, the transition was difficult for the IT team, who had to deal with a security incident not long after transitioning to the e commerce model. After investigating the incident, the team concluded that due to the out-of-date anti-malware software, an attacker gamed access to their files and exposed customers' information, including their names and home addresses.

The IT team decided to stop using the old anti-malware software and install a new one which would automatically remove malicious code in case of similar incidents. The new software was installed in every workstation within the company. After installing the new software, the team updated it with the latest malware definitions and enabled the automatic update feature to keep it up to date at all times. Additionally, they established an authentication process that requires a user identification and password when accessing sensitive information.

In addition, Beauty conducted a number of information security awareness sessions for the IT team and other employees that have access to confidential information in order to raise awareness on the importance of system and network security.

According to scenario 2. Beauty has reviewed all user access rights. What type of control is this?

- A: Detective and administrative
- B: Corrective and managerial
- C: Legal and technical

**Correct Answer: A**

### **Explanation:**

**Preventive controls:** These are controls that aim to prevent or deter the occurrence of a security incident or reduce its likelihood. Examples of preventive controls are encryption, firewalls, locks, policies, etc.

**Detective controls:** These are controls that aim to detect or discover the occurrence of a security incident or its symptoms. Examples of detective controls are logs, alarms, audits, etc.

**Corrective controls:** These are controls that aim to correct or restore the normal state of an asset or a process after a security incident or mitigate its impact. Examples of corrective controls are backups, recovery plans, incident response teams, etc.

**Administrative controls:** These are controls that involve the management and governance of information security, such as policies, procedures, roles, responsibilities, awareness, training, etc.

**Technical controls:** These are controls that involve the use of technology or software to implement information security, such as encryption, firewalls, anti-malware, authentication, etc.

**Physical controls:** These are controls that involve the protection of physical assets or locations from unauthorized access, damage, or theft, such as locks, fences, cameras, guards, etc.

**Legal controls:** These are controls that involve the compliance with laws, regulations, contracts, or agreements related to information security, such as privacy laws, data protection laws, confidentiality agreements, etc.

In scenario 2, the action of Beauty reviewing all user access rights is best described as a "Preventive and Administrative" control.

**Preventive Control:** The review of user access rights is a preventive measure. It is designed to prevent unauthorized access to sensitive information by ensuring that only authorized personnel have access to specific files. By controlling access rights, the organization aims to prevent potential security breaches and protect sensitive data.

**Administrative Control:** This action also falls under administrative controls, sometimes referred to as managerial controls. These controls involve policies, procedures, and practices related to the management of the organization and its employees. In this case, the review of access rights is a part of the company's administrative procedures to manage the security of information systems.

ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection — Information security management systems — Requirements

#### Question 5. (Single Select)

Scenario 2: Beauty is a cosmetics company that has recently switched to an e-commerce model, leaving the traditional retail. The top management has decided to build their own custom

platform in-house and outsource the payment process to an external provider operating online payments systems that support online money transfers.

Due to this transformation of the business model, a number of security controls were implemented based on the identified threats and vulnerabilities associated to critical assets. To protect customers' information. Beauty's employees had to sign a confidentiality agreement. In addition, the company reviewed all user access rights so that only authorized personnel can have access to sensitive files and drafted a new segregation of duties chart.

However, the transition was difficult for the IT team, who had to deal with a security incident not long after transitioning to the e commerce model. After investigating the incident, the team concluded that due to the out-of-date anti-malware software, an attacker gamed access to their files and exposed customers' information, including their names and home addresses.

The IT team decided to stop using the old anti-malware software and install a new one which would automatically remove malicious code in case of similar incidents. The new software was installed in every workstation within the company. After installing the new software, the team updated it with the latest malware definitions and enabled the automatic update feature to keep it up to date at all times. Additionally, they established an authentication process that requires a user identification and password when accessing sensitive information.

In addition, Beauty conducted a number of information security awareness sessions for the IT team and other employees that have access to confidential information in order to raise awareness on the importance of system and network security.

Based on scenario 2, Beauty should have implemented (1)\_\_\_\_\_ to detect (2)\_\_\_\_\_.

A: (1) An access control software, (2) patches

B: (1) Network intrusions, (2) technical vulnerabilities

C: (1) An intrusion detection system, (2) intrusions on networks

**Correct Answer: C**

### **Explanation:**

An intrusion detection system (IDS) is a device or software application that monitors network activities, looking for malicious behaviors or policy violations, and reports their findings to a management station. An IDS can help an organization to detect intrusions on networks, which are unauthorized attempts to access, manipulate, or harm network resources or data. In the scenario, Beauty should have implemented an IDS to detect intrusions on networks, such as the

one that exposed customers' information due to the out-of-date anti-malware software. An IDS could have alerted the IT team about the suspicious network activity and helped them to respond faster and more effectively. Therefore, the correct answer is C.



Full version is available at link below with affordable price.

<https://www.directcertify.com/pecb/iso-iec-27001-lead-implementer>

30% Discount Coupon Code: LimitedTime2025

This is a promotional banner for 'DirectCertify Certification Exams Study Guides'. The background is dark with a large yellow arrow pointing right. On the left, there's a man in a light blue shirt looking thoughtful. A red 'PDF' icon and a 'FREE TRIAL' badge are also present. The main text in large yellow letters reads 'CERTIFICATION EXAMS STUDY GUIDES'. Above this, it says '\* 100% MONEY BACK GUARANTEED'. To the right, a hand is shown holding a fan of US dollar bills. Below the main title, a list of 'Product Features' is provided: '\* 100% Success in the Final Exam', '\* 90 Days Free Updates', '\* Latest Exam Q/A', '\* 24/7 Customer Support', and '\* Practice Exams'. At the bottom, it offers a '\* Free Demo for Practice Test &amp; PDF'. On the right side, there's a box stating '50K Plus Satisfied Customers' and three circular images showing people in professional settings. At the very bottom right, logos for VISA, AMERICAN EXPRESS, DISCOVER, and G Pay are displayed.